Uptick Pty Ltd
398 Johnston Street, Abbotsford VIC 3067

P 1300 657 436
E info@uptickhq.com
W www.uptickhq.com

Data Protection Addendum (GDPR)

1. Definitions

a. In this DPA:

"**Adequate Country**" means a country or territory recognised as providing an adequate level of protection for Personal Data under an adequacy decision made, from time to time, by (as applicable) (i) the Information Commissioner's Office and/or under applicable UK law (including the UK GDPR), or (ii) the European Commission under the GDPR.

"**Data Subject Request**" means a request from or on behalf of a data subject to exercise any rights in relation to their Personal Data under Data Protection Laws.

"**EEA**" means the European Economic Area and Switzerland.

"**Model Clauses**" means the model clauses for the transfer of personal data to processors established in third countries approved by under applicable law and attached as Schedule 1 to this DPA.

"**Personal Data**" means all personal data which is uploaded into the Uptick's products or services by Customer and accessed, stored or otherwise processed by Uptick as a processor.

"**Services**" means the services provided by Uptick to Customer under the agreement, including, as applicable, the Contract Details, Additional Services, and Support Level Agreement.

"**Security Breach**" means any breach of security or other action or inaction leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data by any of Uptick's staff or sub-processors, or any other identified or unidentified third party;

"**Supervisory Authority**" means in the UK, the Information Commissioner's Office ("**ICO**") (and, where applicable, the Secretary of State or the government), and in the EEA, an independent public authority established pursuant to the GDPR.

"**UK**" means the United Kingdom.

"**controller**", "**data subject**", "**personal data**" and "**processor**" have the meanings ascribed to them in the Data Protection Laws.

b. Any defined terms which are not defined in this DPA are as defined in the agreement.

1.2 Roles & compliance with Data Protection Laws

a. Customer is the controller of Personal Data, and Uptick is the processor of Personal Data.

b. Each party will comply (and will procure that any of its personnel comply and use commercially reasonable efforts to procure that its sub-processors comply), with Data Protection Laws applicable to Personal Data. As between the parties, Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which the Personal Data was acquired by the Customer, such that the processing described hereunder may be lawfully undertaken by Customer and Uptick.

c. Each party shall appoint an individual within its organisation authorised to respond from time to time to enquiries regarding the Personal Data and each party shall deal with such enquiries promptly.

2. Description of Processing

a. **Subject Matter of the Processing**: Uptick's provision of the Services to Customer, including the processing of Personal Data.

b. **Nature and Purposes of the Processing**. The nature and purposes of the processing is the collection, storage, duplication, deletion, analysis and disclosure of Personal Data pursuant to providing the Services to Customer and any further instructions by Customer in writing.

c. **Duration of Processing**. Uptick will process the Personal Data for the duration of the Agreement, or until the processing is no longer necessary for the purposes described in this Agreement.

d. **Types of Data**. Any Personal Data that Customer in its discretion uploads into the Services will be processed under this DPA. Customer may not upload special category data.

e. **Categories of Data Subjects**. Data Subjects may include any end users (including without limitation employees, customers, or suppliers) about whom Personal Data is provided to Uptick via the Services by, or at the direction of, Customer.

f. **Processing by Uptick.** Uptick will only process Personal Data (i) in order to provide the Services to Customer or (ii) per Customer's instructions in writing or via the Services. Uptick will notify Customer (unless prohibited by applicable law) if it is required under applicable law to process Personal Data other than pursuant to Customer's instructions. As soon as reasonably practicable upon becoming aware, inform the Customer if, in Uptick's opinion, any instructions provided by the Customer under clause a infringe the GDPR or UK GDPR.

3. Technical and organisational security measures

a. Uptick will implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks that are presented by the processing of Personal Data, in particular protection against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data. Such measures include, without limitation, the security measures set out https://www.uptickhq.com/policies/data-security-framework/.

b. Uptick will take reasonable steps to ensure that only authorised personnel have access to Personal Data and that any persons whom it authorizes to access the Personal Data are under obligations of confidentiality.

4. Security Breaches, Data Subject Requests & Further Assistance

4.1 Security Breaches.

a. Uptick will notify Customer of any Security Breach without undue delay.

4.2 Data Subject Requests.

a. Uptick will promptly notify Customer if it receives a Data Subject Request. Uptick will not respond to a Data Subject Request, provided that Customer agrees Uptick may at its discretion respond to confirm that such request relates to Customer. Customer acknowledges and agrees that the Services include features which will allow Customer to manage Data Subject Requests directly through the Services without additional assistance from Uptick. If Customer does not have the ability to address a Data Subject Request, Uptick will, upon Customer's written request, provide reasonable assistance to facilitate Customer's response to the Data Subject Request to the extent such assistance is consistent with applicable law; provided that Customer will be responsible for paying for any costs incurred or fees charged by Uptick for providing such assistance.

4.3 Further Assistance.

a. Taking into account the nature of processing and the information available to Uptick, Uptick will provide such assistance as Customer reasonably requests in relation to Customer's obligations under Data Protection Laws with respect to (i) data protection impact assessments, (ii) notifications to the Supervisory Authority under Data Protection Laws and/or communications to data subjects by the Customer in response to a Security Breach, or (iii) Customer's compliance with its obligations under the GDPR or UK GDPR (as applicable) with respect to the security of processing. Customer will pay any costs or fees charged by Uptick for providing the assistance in this Section 4.3.

4.4 Sub-processing

a. Customer grants a general authorisation to Uptick to appoint its Affiliates or third parties as sub-processors to support the performance of the Services, including data centre operators, cloud-based software providers, and other outsourced support and service providers. Uptick will maintain a list of sub-processors at the following URL: https://www.uptickhq.com/policies/subprocessors/ and will add the names of new and replacement sub-processors to the list thirty (30) days prior to them starting sub-processing of Personal Data. Customer may subscribe to updates to this list and Uptick will consider any of Customer's reasonable objections to a new sub-processor. If Customer has a reasonable objection to any new or replacement sub-processor and there is no option available for Customer to utilise the Services without use of that sub-processor, Customer's sole and exclusive remedy is to terminate the Agreement, only in relation to the Services to which the proposed new sub-processor's processing of Personal Data relates or would relate, by providing written notice to Uptick.

b. Uptick will enter into a written contract with each sub-processor which imposes on such sub-processor terms no less protective of Personal Data than those imposed on Uptick in this DPA (the "**Relevant Terms**"). Uptick shall be liable to Customer for any breach by such sub-processor of any of the Relevant Terms to the extent required under Data Protection Law.

5. International Transfers

5.1 Data Transfers.

a. Customer agrees that its use of the Services may involve the transfer of Personal Data to, and processing of Personal Data in, locations outside of the UK and/or EEA from time to time, such as for purposes of providing support to Customer, including processing in Australia, New Zealand, and the United States.

b. To the extent Uptick processes Personal Data outside the UK or EEA (except if in an Adequate Country), the parties agree that the Model Clauses will apply and are incorporated into this DPA, and Uptick is the 'data importer' and will comply with the obligations of the 'data importer' in the Model Clauses accordingly and Customer is the 'data exporter' and will comply with the obligations of the 'data exporter' accordingly. The following terms shall apply to the Model Clauses:

c. Clause 2 of this DPA contain the information required by Annexes 1 & 2 of the Model Clauses.

   i. Customer may exercise its right of audit under clause 5(f) of the Model Clauses as set out in, and subject to the requirements of, clause 6 of this DPA;

   ii. Uptick may appoint sub-processors as set out, and subject to the requirements of, clause 4.4 of this DPA.

d. Uptick may (i) replace the Model Clauses generally or in respect of the UK and/or the EEA only (as appropriate) with any alternative or replacement transfer mechanism in compliance with applicable Data Protection Laws, including any standard contractual clauses approved by an applicable Supervisory Authority, and (ii) make reasonably necessary changes to this clause 5 by notifying Customer of the new transfer mechanism or content of the new Model Clauses (provided their content is in compliance with the relevant decision or approval), as applicable.

6. Audit and Records

a. Uptick will, subject to the confidentiality terms in the Agreement, provide Customer such information in Uptick's possession or control as may be necessary to demonstrate compliance with its obligations under this DPA. The Customer may exercise its right of audit under Data Protection Laws, through Uptick providing:

i. an audit report not older than 18 months by a registered and independent external auditor demonstrating that Uptick's technical and organizational measures are sufficient and in accordance with an accepted industry audit standard (ISO 27001), and

ii. additional information in Uptick's possession or control to a Supervisory Authority when it requests or requires additional information in relation to the data processing activities carried out by Uptick under this DPA.

7. Deletion or return of data

Upon termination of this Agreement, Uptick will delete the Personal Data as soon as reasonably practicable and no later than thirty (30) days following such termination and Customer may download the Personal Data any time prior to it being deleted. Notwithstanding the foregoing, Uptick may retain Personal Data beyond termination solely if, and for so long as, such Personal Data must be retained in order to comply with applicable law.

8. Conflicts.

This DPA is without prejudice to the rights and obligations of the parties under the Agreement which shall continue to have full force and effect. In the event of any conflict between the terms of this DPA and the terms of the Agreement, the terms (including definitions) of this DPA shall prevail so far as the subject matter concerns the processing of Personal Data. This DPA sets out all of the terms that have been agreed between the parties in relation to the subjects covered by it. Other than in respect of statements made fraudulently, no other representations or terms shall apply or form part of this DPA.

MODEL CLAUSES

2010 EU Model clauses extracted from 2010/87/EU Annex EU Standard Contractual Clauses for the transfer of personal data to data processors established in third countries which do not ensure an adequate level of data protection

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Uptick and Customer, each a '**party**'; together '**the parties**',

HAVE AGREED on the following Contractual Clauses (the '**Clauses**') in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) '**personal data**', '**special categories of data**', '**process/processing**', '**controller**', '**processor**', '**data subject**' and '**supervisory authority**' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

the '**data exporter**' means the controller who transfers the personal data;

the '**data importer**' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

the '**sub-processor**' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

the '**applicable data protection law**' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established; and

'**technical and organisational security measures**' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter’s behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing law

The Clauses shall be governed by the laws of the state of New York.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data

exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the laws of the state of New York.

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.